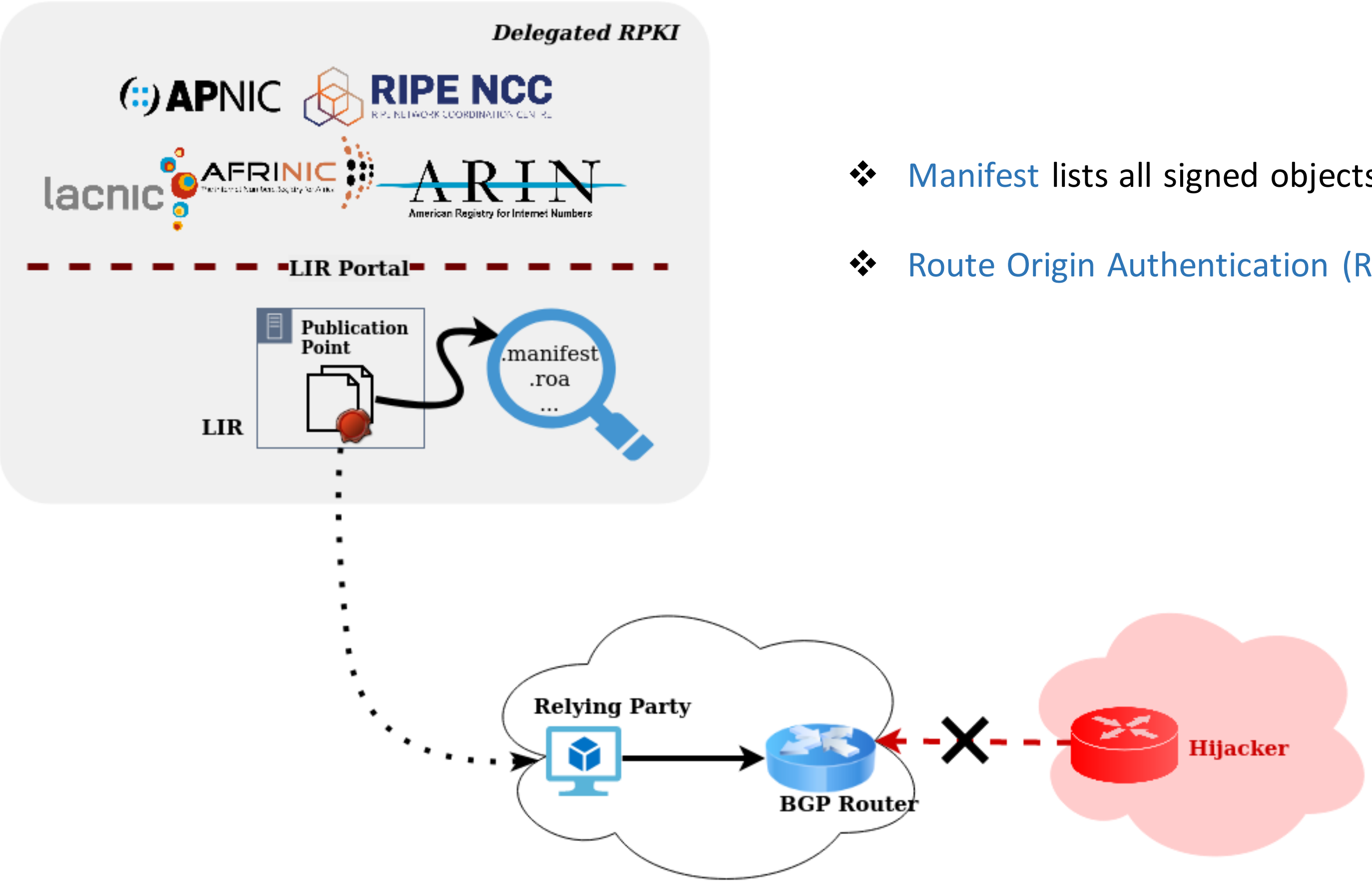
Stalloris:
RPKI Downgrade Attack

Tomas Hlavacek, Philipp Jeitner, **Donika Mirdita**, Haya Shulman and Michael Waidner

German National Research Center for Applied Cybersecurity ATHENE
Fraunhofer Institute for Secure Information Technology SIT
Technical University Darmstadt
Goethe-University Frankfurt

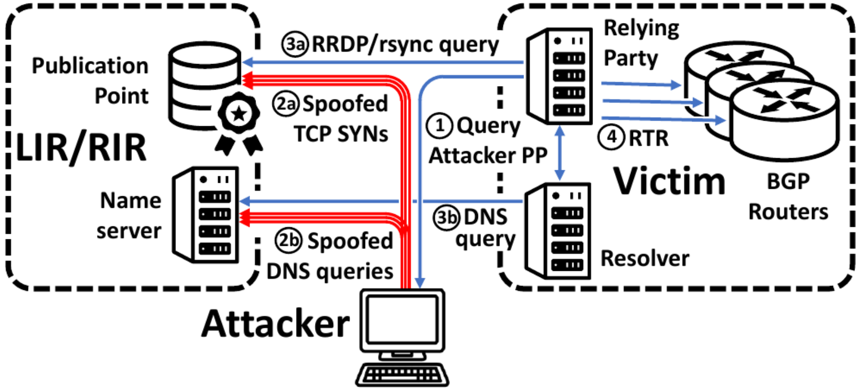
A Short Introduction to RPKI



- Manifest lists all signed objects in Publication Point repository
- Route Origin Authentication (ROA) signed pair of (IP Prefix Block, ASN)

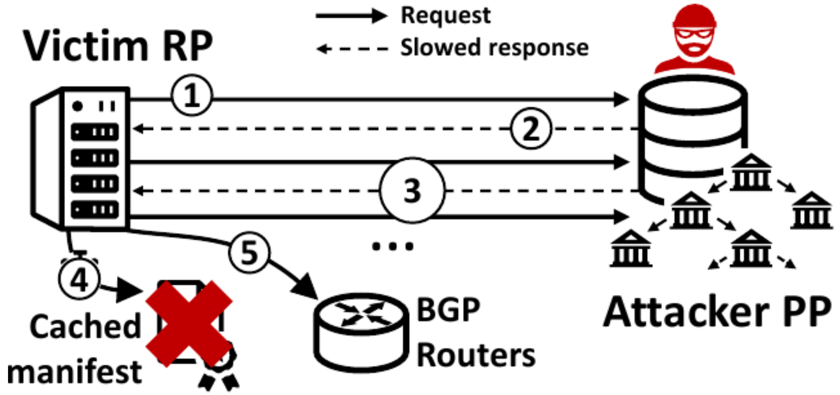
Downgrade RPKI: Low-Rate Attack

1. Relying Party (RP) connects to the attacker's Publication Points (PP)
2. Attacker makes target PP unreachable via rate-limiting
   a. Spoof TCP SYN packets to overload PP
   b. Spoof DNS queries to nameserver
3. Queries from RP and its resolvers go unanswered, repeat periodically until
4. Objects in RP cache expire
   a. ROAs of target PP are no longer available
   b. BGP Router gets incomplete data => RPKI Downgrade



[Optimized] Downgrade RPKI: Stalloris

1. Victim RP sends request to Attacker PP
2. Attacker PP stalls the victim RP until **timeout**
3. Victim RP traverses the delegation tree of the attacker
   - Stalling time is **size_of_tree x timeout**
4. Stalling persists until cached manifest times out
5. ROAs from expired manifests no longer available
   - Route RPKI status in router switches: *Valid -> Not Found*



Vulnerabilities in the RPKI Environment

Rate-Limiting in DNS

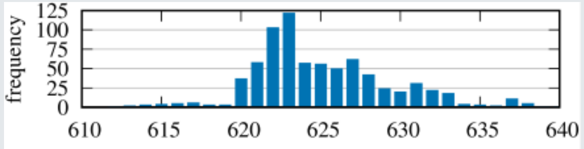
- Rate-limiting in nameservers & PPs

responses/s	3	4	445	1137	1142	1146	1146	1207	1212
answers/s	3	2	82	1137	1142	1146	1146	1207	1212
responses/s	1223	1287	1288	1296	1308	1309	1520	1642	2621
answers/s	1223	1287	1288	1296	1308	1309	12	1301	1236
responses/s	3248	3248	4000	∞	∞	∞	∞	-	-
answers/s	16	16	88	3	7	7	7	-	-

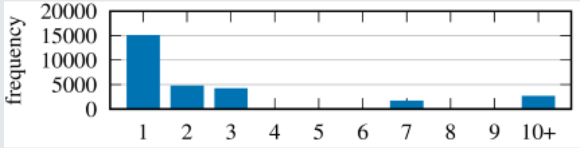
- 47% of PPs vulnerable
- 20.4% of IPv4 space vulnerable

RP Predictability

- Regular refresh intervals (ex. Routinator)

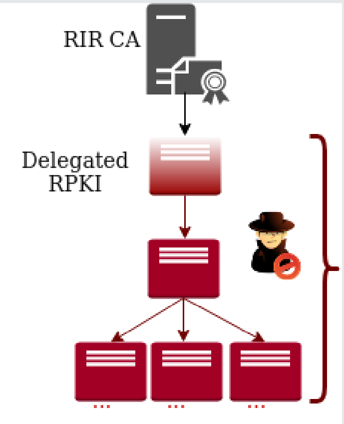


- 70% of MFTs < 48h validity



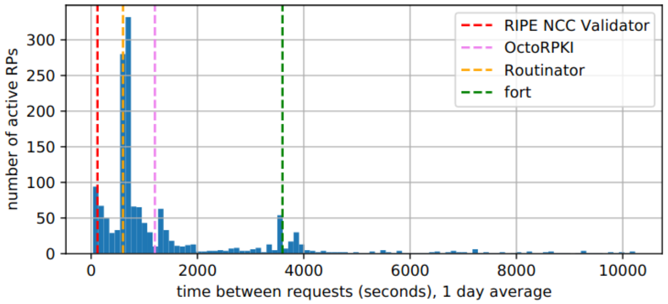
Unlimited Delegation Chain

- Infinite (re-)delegation of same resources



Attack Feasibility

Refresh Intervals for RPs are deterministic

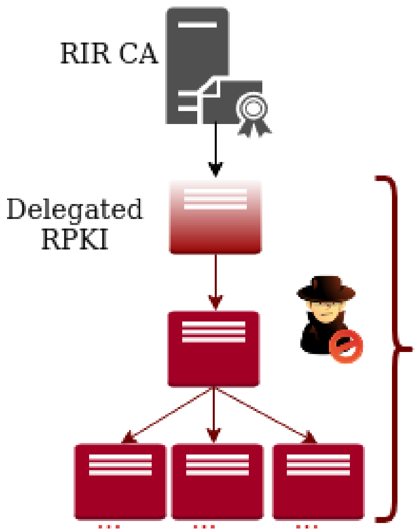


Packet volume for successful attack

(Scenario)	$n_{attempts}$	t_{attack}	t_{sleep}	$n_{retries}$	o
(1)	24	old manifest 6 *hours*	unbound (blocked) 900 *s*	unbound (blocked) 1	35
(2)	864	fresh manifest 1 *day*	routinator (normal) 600 *s*	bind9 / linux tcp 6	1247
(3)	23040	long-valid manifest 2 *days*	RIPE NCC validator 120 *s*	unbound normal 16	33240
(S)	55	fresh manifest 1 *day*	routinator (stalled) 2.6 *hours*	bind9 / linux tcp 6	80

(Scenario) o	r_{limit}	$r_{attacker}$
(1) 35	3 60 1288	105 2,100 45,080
(2) 1247	3 60 1288	3,741 74,820 1,606,136
(3) 33240	3 60 1288	99,720 1,994,400 42,813,120
(S) 80	3 60 1288	240 4,800 103,040

Open Source Software to build attacker's malicious Repo Tree



Results

- Rate-Limiting affects almost half of all Publication Points
- An attacker has all the available open source tools necessary to do an optimized Stalloris Rate-Limiting attack
- Relying Party do not provide feedback when something abnormal is happening: Stalloris can only be detected via manual log checking
- Attack effectively bypasses RPKI protection of prefixes despite RPKI being correctly implemented by client and user alike

Thank you for your attention!

If you have any questions, contact at

donika.mirdita@sit.fraunhofer.de

תודה רבה!

çok teşekkürler

谢谢

Merci beaucoup!

Thank you very much!

Dank je wel!

Vielen Dank!

Muchas gracias

ありがとうございました

Dziękuję!

zor spas

Grazie mille!

اشكرك